

AMENDED IN SENATE MAY 6, 2014
AMENDED IN SENATE APRIL 29, 2014
AMENDED IN SENATE APRIL 9, 2014

SENATE BILL

No. 893

Introduced by Senator Hill

January 13, 2014

An act to amend Sections 1798.29 and 1798.82 of, and to add Title 1.81.23 (commencing with Section 1798.90.5) to Part 4 of Division 3 of, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 893, as amended, Hill. Automated license plate recognition systems: use of data.

(1) Existing law authorizes the Department of the California Highway Patrol to retain license plate data captured by license plate recognition (LPR) technology, also referred to as an automated license plate recognition (ALPR) system, for not more than 60 days unless the data is being used as evidence or for the investigation of felonies. Existing law prohibits the department from selling the data or from making the data available to an agency that is not a law enforcement agency or an individual that is not a law enforcement officer.

Existing law authorizes the department to use LPR data for the purpose of locating vehicles or persons reasonably suspected of being involved in the commission of a public offense, and requires the department to monitor the internal use of the data to prevent unauthorized use and to submit to the Legislature, as a part of the annual automobile theft report, information on the department's LPR practices and usage.

This bill would impose specified requirements on an “ALPR operator,” as defined, including, among others, complying with all applicable statutory and constitutional requirements and the provisions of the bill, ensuring that the information or data the ALPR operator collects is protected with certain safeguards, and to implement and maintain specified security procedures and a usage and privacy policy with respect to that information or data.

This bill would also prohibit an ALPR operator from engaging in certain acts, including, among others, retaining any information or data other than the license plate number, the date and time the information or data is collected, and the location coordinates where the information or data is collected. The bill would further prohibit a public agency from disclosing, distributing, making available, selling, accessing, or otherwise providing that information or data, to any private entity or individual unless authorized by a court order, or as part of civil or criminal discovery. Unless otherwise authorized, the bill would prohibit a person authorized to access or distribute that information or data from further disclosing, distributing, making available, selling, accessing, or otherwise providing that information or data to another person for any purpose. The bill would require an ALPR operator that accesses or provides access to information or data collected through the use or operation of an ALPR system to maintain a specified record of that access.

The bill would, in addition to any other sanctions, penalties, or remedies provided by law, authorize an individual to bring a civil action in any court of competent jurisdiction against a person who knowingly obtains, discloses, or uses information or data collected through the use of an ALPR system in violation of the bill, and would authorize a court to award specified remedies.

(2) Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law defines “personal information” for these purposes to include an individual’s first name and last name, or first initial and last name, in combination with one or more designated data elements

relating to, among other things, social security numbers, driver’s license numbers, financial accounts, and medical information.

This bill would include information or data collected through the use or operation of an automated license plate recognition system, when that information or data is not encrypted, in the definition of “personal information” discussed above. ~~By creating new duties for local officials, the bill would impose a state-mandated local program.~~

~~The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.~~

~~This bill would provide that, if the Commission on State Mandates determines that the bill contains costs mandated by the state, reimbursement for those costs shall be made pursuant to these statutory provisions.~~

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: ~~yes~~-no.

The people of the State of California do enact as follows:

1 SECTION 1. Section 1798.29 of the Civil Code is amended
2 to read:

3 1798.29. (a) Any agency that owns or licenses computerized
4 data that includes personal information shall disclose any breach
5 of the security of the system following discovery or notification
6 of the breach in the security of the data to any resident of California
7 whose unencrypted personal information was, or is reasonably
8 believed to have been, acquired by an unauthorized person. The
9 disclosure shall be made in the most expedient time possible and
10 without unreasonable delay, consistent with the legitimate needs
11 of law enforcement, as provided in subdivision (c), or any measures
12 necessary to determine the scope of the breach and restore the
13 reasonable integrity of the data system.

14 (b) Any agency that maintains computerized data that includes
15 personal information that the agency does not own shall notify the
16 owner or licensee of the information of any breach of the security
17 of the data immediately following discovery, if the personal
18 information was, or is reasonably believed to have been, acquired
19 by an unauthorized person.

20 (c) The notification required by this section may be delayed if
21 a law enforcement agency determines that the notification will

1 impede a criminal investigation. The notification required by this
2 section shall be made after the law enforcement agency determines
3 that it will not compromise the investigation.

4 (d) Any agency that is required to issue a security breach
5 notification pursuant to this section shall meet all of the following
6 requirements:

7 (1) The security breach notification shall be written in plain
8 language.

9 (2) The security breach notification shall include, at a minimum,
10 the following information:

11 (A) The name and contact information of the reporting agency
12 subject to this section.

13 (B) A list of the types of personal information that were or are
14 reasonably believed to have been the subject of a breach.

15 (C) If the information is possible to determine at the time the
16 notice is provided, then any of the following: (i) the date of the
17 breach, (ii) the estimated date of the breach, or (iii) the date range
18 within which the breach occurred. The notification shall also
19 include the date of the notice.

20 (D) Whether the notification was delayed as a result of a law
21 enforcement investigation, if that information is possible to
22 determine at the time the notice is provided.

23 (E) A general description of the breach incident, if that
24 information is possible to determine at the time the notice is
25 provided.

26 (F) The toll-free telephone numbers and addresses of the major
27 credit reporting agencies, if the breach exposed a social security
28 number or a driver's license or California identification card
29 number.

30 (3) At the discretion of the agency, the security breach
31 notification may also include any of the following:

32 (A) Information about what the agency has done to protect
33 individuals whose information has been breached.

34 (B) Advice on steps that the person whose information has been
35 breached may take to protect himself or herself.

36 (4) In the case of a breach of the security of the system involving
37 personal information defined in paragraph (2) of subdivision (g)
38 for an online account, and no other personal information defined
39 in paragraph (1) of subdivision (g), the agency may comply with
40 this section by providing the security breach notification in

1 electronic or other form that directs the person whose personal
2 information has been breached to promptly change his or her
3 password and security question or answer, as applicable, or to take
4 other steps appropriate to protect the online account with the
5 agency and all other online accounts for which the person uses the
6 same user name or email address and password or security question
7 or answer.

8 (5) In the case of a breach of the security of the system involving
9 personal information defined in paragraph (2) of subdivision (g)
10 for login credentials of an email account furnished by the agency,
11 the agency shall not comply with this section by providing the
12 security breach notification to that email address, but may, instead,
13 comply with this section by providing notice by another method
14 described in subdivision (i) or by clear and conspicuous notice
15 delivered to the resident online when the resident is connected to
16 the online account from an Internet Protocol address or online
17 location from which the agency knows the resident customarily
18 accesses the account.

19 (e) Any agency that is required to issue a security breach
20 notification pursuant to this section to more than 500 California
21 residents as a result of a single breach of the security system shall
22 electronically submit a single sample copy of that security breach
23 notification, excluding any personally identifiable information, to
24 the Attorney General. A single sample copy of a security breach
25 notification shall not be deemed to be within subdivision (f) of
26 Section 6254 of the Government Code.

27 (f) For purposes of this section, “breach of the security of the
28 system” means unauthorized acquisition of computerized data that
29 compromises the security, confidentiality, or integrity of personal
30 information maintained by the agency. Good faith acquisition of
31 personal information by an employee or agent of the agency for
32 the purposes of the agency is not a breach of the security of the
33 system, provided that the personal information is not used or
34 subject to further unauthorized disclosure.

35 (g) For purposes of this section, “personal information” means
36 any of the following:

37 (1) An individual’s first name or first initial and last name in
38 combination with any one or more of the following data elements,
39 when either the name or the data elements are not encrypted:

40 (A) Social security number.

1 (B) Driver’s license number or California identification card
2 number.

3 (C) Account number, credit or debit card number, in
4 combination with any required security code, access code, or
5 password that would permit access to an individual’s financial
6 account.

7 (D) Medical information.

8 (E) Health insurance information.

9 (2) A user name or email address, in combination with a
10 password or security question and answer that would permit access
11 to an online account.

12 (3) Information or data collected through the use or operation
13 of an automated license plate recognition system, as defined in
14 Section 1798.90.5, when that information or data is not encrypted.

15 (h) (1) For purposes of this section, “personal information”
16 does not include publicly available information that is lawfully
17 made available to the general public from federal, state, or local
18 government records.

19 (2) For purposes of this section, “medical information” means
20 any information regarding an individual’s medical history, mental
21 or physical condition, or medical treatment or diagnosis by a health
22 care professional.

23 (3) For purposes of this section, “health insurance information”
24 means an individual’s health insurance policy number or subscriber
25 identification number, any unique identifier used by a health insurer
26 to identify the individual, or any information in an individual’s
27 application and claims history, including any appeals records.

28 (i) For purposes of this section, “notice” may be provided by
29 one of the following methods:

30 (1) Written notice.

31 (2) Electronic notice, if the notice provided is consistent with
32 the provisions regarding electronic records and signatures set forth
33 in Section 7001 of Title 15 of the United States Code.

34 (3) Substitute notice, if the agency demonstrates that the cost
35 of providing notice would exceed two hundred fifty thousand
36 dollars (\$250,000), or that the affected class of subject persons to
37 be notified exceeds 500,000 *persons*, or the agency does not have
38 sufficient contact information. Substitute notice shall consist of
39 all of the following:

1 (A) Email notice when the agency has an email address for the
2 subject persons.

3 (B) Conspicuous posting of the notice on the agency’s Internet
4 Web site page, if the agency maintains one.

5 (C) Notification to major statewide media and the Office of
6 Information Security within the Department of Technology.

7 (j) Notwithstanding subdivision (i), an agency that maintains
8 its own notification procedures as part of an information security
9 policy for the treatment of personal information and is otherwise
10 consistent with the timing requirements of this part shall be deemed
11 to be in compliance with the notification requirements of this
12 section if it notifies subject persons in accordance with its policies
13 in the event of a breach of security of the system.

14 (k) Notwithstanding the exception specified in paragraph (4) of
15 subdivision (b) of Section 1798.3, for purposes of this section,
16 “agency” includes a local agency, as defined in subdivision (a) of
17 Section 6252 of the Government Code.

18 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

19 1798.82. (a) Any person or business that conducts business
20 in California, and that owns or licenses computerized data that
21 includes personal information, shall disclose any breach of the
22 security of the system following discovery or notification of the
23 breach in the security of the data to any resident of California
24 whose unencrypted personal information was, or is reasonably
25 believed to have been, acquired by an unauthorized person. The
26 disclosure shall be made in the most expedient time possible and
27 without unreasonable delay, consistent with the legitimate needs
28 of law enforcement, as provided in subdivision (c), or any measures
29 necessary to determine the scope of the breach and restore the
30 reasonable integrity of the data system.

31 (b) Any person or business that maintains computerized data
32 that includes personal information that the person or business does
33 not own shall notify the owner or licensee of the information of
34 any breach of the security of the data immediately following
35 discovery, if the personal information was, or is reasonably
36 believed to have been, acquired by an unauthorized person.

37 (c) The notification required by this section may be delayed if
38 a law enforcement agency determines that the notification will
39 impede a criminal investigation. The notification required by this

1 section shall be made after the law enforcement agency determines
2 that it will not compromise the investigation.

3 (d) Any person or business that is required to issue a security
4 breach notification pursuant to this section shall meet all of the
5 following requirements:

6 (1) The security breach notification shall be written in plain
7 language.

8 (2) The security breach notification shall include, at a minimum,
9 the following information:

10 (A) The name and contact information of the reporting person
11 or business subject to this section.

12 (B) A list of the types of personal information that were or are
13 reasonably believed to have been the subject of a breach.

14 (C) If the information is possible to determine at the time the
15 notice is provided, then any of the following: (i) the date of the
16 breach, (ii) the estimated date of the breach, or (iii) the date range
17 within which the breach occurred. The notification shall also
18 include the date of the notice.

19 (D) Whether notification was delayed as a result of a law
20 enforcement investigation, if that information is possible to
21 determine at the time the notice is provided.

22 (E) A general description of the breach incident, if that
23 information is possible to determine at the time the notice is
24 provided.

25 (F) The toll-free telephone numbers and addresses of the major
26 credit reporting agencies if the breach exposed a social security
27 number or a driver's license or California identification card
28 number.

29 (3) At the discretion of the person or business, the security
30 breach notification may also include any of the following:

31 (A) Information about what the person or business has done to
32 protect individuals whose information has been breached.

33 (B) Advice on steps that the person whose information has been
34 breached may take to protect himself or herself.

35 (4) In the case of a breach of the security of the system involving
36 personal information defined in paragraph (2) of subdivision (h)
37 for an online account, and no other personal information defined
38 in paragraph (1) of subdivision (h), the person or business may
39 comply with this section by providing the security breach
40 notification in electronic or other form that directs the person whose

1 personal information has been breached promptly to change his
2 or her password and security question or answer, as applicable, or
3 to take other steps appropriate to protect the online account with
4 the person or business and all other online accounts for which the
5 person whose personal information has been breached uses the
6 same user name or email address and password or security question
7 or answer.

8 (5) In the case of a breach of the security of the system involving
9 personal information defined in paragraph (2) of subdivision (h)
10 for login credentials of an email account furnished by the person
11 or business, the person or business shall not comply with this
12 section by providing the security breach notification to that email
13 address, but may, instead, comply with this section by providing
14 notice by another method described in subdivision (j) or by clear
15 and conspicuous notice delivered to the resident online when the
16 resident is connected to the online account from an Internet
17 Protocol address or online location from which the person or
18 business knows the resident customarily accesses the account.

19 (e) A covered entity under the federal Health Insurance
20 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d
21 et seq.) will be deemed to have complied with the notice
22 requirements in subdivision (d) if it has complied completely with
23 Section 13402(f) of the federal Health Information Technology
24 for Economic and Clinical Health Act (Public Law 111-5).
25 However, nothing in this subdivision shall be construed to exempt
26 a covered entity from any other provision of this section.

27 (f) Any person or business that is required to issue a security
28 breach notification pursuant to this section to more than 500
29 California residents as a result of a single breach of the security
30 system shall electronically submit a single sample copy of that
31 security breach notification, excluding any personally identifiable
32 information, to the Attorney General. A single sample copy of a
33 security breach notification shall not be deemed to be within
34 subdivision (f) of Section 6254 of the Government Code.

35 (g) For purposes of this section, “breach of the security of the
36 system” means unauthorized acquisition of computerized data that
37 compromises the security, confidentiality, or integrity of personal
38 information maintained by the person or business. Good faith
39 acquisition of personal information by an employee or agent of
40 the person or business for the purposes of the person or business

1 is not a breach of the security of the system, provided that the
2 personal information is not used or subject to further unauthorized
3 disclosure.

4 (h) For purposes of this section, “personal information” means
5 any of the following:

6 (1) An individual’s first name or first initial and last name in
7 combination with any one or more of the following data elements,
8 when either the name or the data elements are not encrypted:

9 (A) Social security number.

10 (B) Driver’s license number or California identification card
11 number.

12 (C) Account number, credit or debit card number, in
13 combination with any required security code, access code, or
14 password that would permit access to an individual’s financial
15 account.

16 (D) Medical information.

17 (E) Health insurance information.

18 (2) A user name or email address, in combination with a
19 password or security question and answer that would permit access
20 to an online account.

21 (3) Information or data collected through the use or operation
22 of an automated license plate recognition system, as defined in
23 Section 1798.90.5, when that information or data is not encrypted.

24 (i) (1) For purposes of this section, “personal information” does
25 not include publicly available information that is lawfully made
26 available to the general public from federal, state, or local
27 government records.

28 (2) For purposes of this section, “medical information” means
29 any information regarding an individual’s medical history, mental
30 or physical condition, or medical treatment or diagnosis by a health
31 care professional.

32 (3) For purposes of this section, “health insurance information”
33 means an individual’s health insurance policy number or subscriber
34 identification number, any unique identifier used by a health insurer
35 to identify the individual, or any information in an individual’s
36 application and claims history, including any appeals records.

37 (j) For purposes of this section, “notice” may be provided by
38 one of the following methods:

39 (1) Written notice.

1 (2) Electronic notice, if the notice provided is consistent with
2 the provisions regarding electronic records and signatures set forth
3 in Section 7001 of Title 15 of the United States Code.

4 (3) Substitute notice, if the person or business demonstrates that
5 the cost of providing notice would exceed two hundred fifty
6 thousand dollars (\$250,000), or that the affected class of subject
7 persons to be notified exceeds 500,000 *persons*, or the person or
8 business does not have sufficient contact information. Substitute
9 notice shall consist of all of the following:

10 (A) Email notice when the person or business has an email
11 address for the subject persons.

12 (B) Conspicuous posting of the notice on the Internet Web site
13 page of the person or business, if the person or business maintains
14 one.

15 (C) Notification to major statewide media.

16 (k) Notwithstanding subdivision (j), a person or business that
17 maintains its own notification procedures as part of an information
18 security policy for the treatment of personal information and is
19 otherwise consistent with the timing requirements of this part, shall
20 be deemed to be in compliance with the notification requirements
21 of this section if the person or business notifies subject persons in
22 accordance with its policies in the event of a breach of security of
23 the system.

24 SEC. 3. Title 1.81.23 (commencing with Section 1798.90.5)
25 is added to Part 4 of Division 3 of the Civil Code, to read:

26
27 TITLE 1.81.23. COLLECTION OF LICENSE PLATE
28 INFORMATION
29

30 1798.90.5. The following definitions shall apply for purposes
31 of this title:

32 (a) “ALPR operator” means a person that uses or operates an
33 ALPR system, or accesses, stores, or maintains information or data
34 collected through the use or operation of an ALPR ~~system~~; *system*,
35 *but does not include the Department of the California Highway*
36 *Patrol when subject to Section 2413 of the Vehicle Code or a*
37 *transportation agency when subject to Section 31490 of the Streets*
38 *and Highways Code.*

39 (b) “Automated license plate recognition system” or “ALPR
40 system” means a system of one or more mobile or fixed cameras

1 combined with computer algorithms to read and convert images
2 of registration plates and the characters they contain into
3 computer-readable data.

4 (c) “Person” includes a law enforcement agency, government
5 agency, private entity, or individual.

6 (d) “Public agency” means and includes every state agency and
7 every local agency.

8 1798.90.51. An ALPR operator shall do all of the following:

9 (a) Comply with all applicable statutory and constitutional
10 requirements and this title.

11 (b) (1) Ensure that the information or data collected through
12 the use or operation of the ALPR system is protected with
13 reasonable operational, administrative, technical, and physical
14 safeguards to ensure its confidentiality and integrity.

15 (2) Implement and maintain reasonable security procedures and
16 practices appropriate for the nature of the information or data
17 collected, in order to protect the information or data from
18 unauthorized access, destruction, use, modification, or disclosure,
19 and to ensure compliance with this title.

20 (c) Implement and maintain a usage and privacy policy in order
21 to ensure that the information or data collected through the use or
22 operation of the ALPR system is consistent with respect for
23 individuals’ privacy and civil liberties. The usage and privacy
24 policy shall be available in writing, and, if the ALPR operator has
25 an Internet Web site, the usage and privacy policy shall be posted
26 conspicuously on that Internet Web site.

27 1798.90.52. An ALPR operator shall not do either of the
28 following:

29 (a) Retain any information or data other than the license plate
30 number, the date and time the information or data is collected, and
31 the location coordinates where the information or data is collected.
32 This information or data shall not be collected if the license plate
33 number is not in public view.

34 (b) (1) Trespass or otherwise enter upon private property to
35 collect information or data for commercial purposes through the
36 use or operation of an ALPR system without first obtaining written
37 consent from the owner of the private property, or the owner’s
38 designated agent.

1 (2) This subdivision shall only apply if the ALPR operator is a
2 private entity that operates an ALPR system for commercial
3 purposes.

4 1798.90.53. (a) A public agency shall not disclose, distribute,
5 make available, sell, access, or otherwise provide for another
6 purpose, information or data collected through the use or operation
7 of an ALPR system to any private entity or individual unless
8 authorized by a court order, or as part of civil or criminal discovery.

9 (b) Unless authorized by this title or another law, a person
10 authorized to access or distribute information or data collected
11 through the use or operation of an ALPR system shall not further
12 disclose, distribute, make available, sell, access, or otherwise
13 provide that information or data to another person for any purpose.

14 (c) If an ALPR operator accesses or provides access to
15 information or data collected through the use or operation of an
16 ALPR system, the ALPR operator shall maintain a record of that
17 access. At a minimum, the record shall include, but not be limited
18 to, all of the following:

19 (1) The date and time the information or data is accessed.

20 (2) The person who accesses the information or data.

21 (3) The purpose for accessing the information or data.

22 1798.90.54. Information or data collected through the use or
23 operation of an ALPR system shall not be the sole basis for
24 establishing probable cause to obtain a search or arrest warrant.

25 1798.90.55. (a) In addition to any other sanctions, penalties,
26 or remedies provided by law, an individual may bring a civil action
27 in any court of competent jurisdiction against a person who
28 knowingly obtains, discloses, or uses information or data collected
29 through the use of an ALPR system in violation of this title.

30 (b) The court may award all of the following:

31 (1) Actual damages, but not less than liquidated damages in the
32 amount of two thousand five hundred dollars (\$2,500).

33 (2) Punitive damages upon proof of willful or reckless disregard
34 of the law.

35 (3) Reasonable attorney's fees and other litigation costs
36 reasonably incurred.

37 (4) Other preliminary and equitable relief as the court determines
38 to be appropriate.

39 ~~SEC. 4. If the Commission on State Mandates determines that~~
40 ~~this act contains costs mandated by the state, reimbursement to~~

1 ~~local agencies and school districts for those costs shall be made~~
2 ~~pursuant to Part 7 (commencing with Section 17500) of Division~~
3 ~~4 of Title 2 of the Government Code.~~

O